SECURE ACCESS MANAGEMENT: A COTS-BASED PROOF-OF-CONCEPT

Dr. S. Zeber*
Defence R&D Canada – Ottawa
Ottawa, ON K1A 0Z4

A. Magar
Magar Security Architecture Inc.
Ottawa, ON K1S 3J7

ABSTRACT

This paper describes the successful demonstration of secure policy-based authorization using commercial products in a content-based information security architecture.

1. INTRODUCTION

The Department of National Defence (DND) currently uses physically separate networks to achieve need-to-know separation in the classified environment based on warning terms, or "caveats", such as CEO (Canadian Eyes Only), CANUS (Canadian-US), and NATO. Using separate networks results in the need to manage user authentication and access privileges based on identity, security clearances, and role authorizations, separately for each network. Such an environment is costly and inefficient to manage, and it inhibits information sharing among users belonging to multiple caveats. System, network, user, and security management necessarily involve duplication of effort and information, and impose a need to synchronize common information across all networks. Furthermore, failure to maintain the synchronization of security attributes and security policies across all networks provides opportunities to compromise security.

2. ARCHITECTURE PROPOSAL

A recent paper (Zeber and Magar, 2002) proposed a "defence-in-depth" architectural model for a content-based approach to information security that protected information based on its content attributes[1] at the point of origin rather than on the security attributes of the network. The proposal advocated the use of commercial off-the-shelf (COTS) products, including operating systems (OS) and public key and privilege management infrastructure[2] (PKI and PMI) technologies based on open standards, with identified enhancements to achieve the desired capability. The combination of OS, PKI and PMI technologies provides a robust basis for security by leveraging their individual strengths, while the enhancements address deficiencies identified in standard COTS implementations of these technologies. A single network environment that included strong authentication, centralized identity management, information labeling, policy-based authorization, and audit, would eliminate the inefficiencies inherent in multiple network environments and would facilitate information sharing while rigorously enforcing security policy requirements.

Two successive secure access management proof-of-concept (SAMPOC) systems, built entirely by integrating commercial products, have now demonstrated the practical viability of this approach, and have provided valuable lessons in the integration of COTS products to provide secure access management. Issues of performance, scalability, ease of use and evaluation and accreditation were beyond the scope of these demonstrators.

3. SAMPOC I

The first SAMPOC system (Magar, 2003) demonstrated a policy-based authorization solution for documents on a file server. The key component of SAMPOC I was the Texar SecureRealms DS[3] policy server, which provided policy-based document encryption and access control (i.e., authorization), and an audit log of all transactions. Entrust PKI v6 with Datakey Smartcards

[1] This is similar to a US initiative known as Content-Based Information Security (CBIS).

[2] In this paper, PMI denotes a comprehensive access management solution, which may not necessarily include the use of attribute certificates.

[3] This product is no longer available.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 DEC 2004	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Secure Access Management: A Cots-Based Proof-Of-Concept	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defence R&D Canada Ottawa Ottawa, ON K1A 0Z4; Magar Security Architecture Inc. Ottawa, ON K1S 3J7**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida. , The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**2**	

provided strong authentication and key management for SecureRealms DS; Access360 enRole[4] provided identity management and provisioning; an Oracle database provided the store for the security policy, secure documents, metadata tags used to label the documents, and the audit logs; and an iPlanet directory, provided an LDAP repository for the Entrust PKI and identity information. The server and workstation platforms were Microsoft Windows NT systems.

SAMPOC I successfully demonstrated policy-based authorization for access to encrypted documents. When an authenticated user requested access to an encrypted document, the SecureRealms policy server evaluated the user's authenticated credentials, including his configured access privileges, the label attached to the requested document, and the security policy, and determined a yes/no answer to the question: "Does the security policy allow the user, described by the associated credentials, access to the requested document with the attached label?" If the answer was yes, then the user was granted access to the protected document, otherwise access was denied. In either case the audit component generated a log entry for the event.

4. SAMPOC II

Using the results and feedback from the SAMPOC I demonstrations, a second demonstrator system, SAMPOC II, (Magar 2004a, 2004b) was built, which extended the policy-based protection mechanism of SAMPOC I to include database and web information as well as documents on a file server. SAMPOC II was implemented on Microsoft Windows 2000/2003 servers and workstations to address a requirement to leverage the native capabilities of those operating systems that comprise the baseline of the DND environment.

SAMPOC I, and SAMPOC II used a comparable but different suite of COTS products. SAMPOC II incorporated a full suite of Entrust products. Entrust Authority and Entrust Entelligence v7.0 provided the PKI services; Entrust GetAccess v7, combined with the Entrust Secure Transaction Platform v7, provided policy-based authorization; Entrust TruePass v7 provided additional certificate-based authentication; and the Sun Identity Manager (formerly Waveset Lighthouse) provided the identity management and provisioning. The system also included Microsoft Windows Rights Management services, an Oracle 9i database, a Samba file server on a Red Hat Linux platform and two custom-developed, policy enforcement point modules.

SAMPOC II successfully demonstrated policy-based authorization for documents, web resources and database entries; labeling approaches for these three types of information objects; the use of XACML to specify authorization policies; the use of SAML assertions to communicate access requests and responses; and the enforcement of security policies for document handling and email messages at the user desktop, using Microsoft Windows Rights Management services.

ACKNOWLEDGEMENTS

Defence R&D Canada gratefully acknowledges the support of Microsoft Canada, Entrust Limited, and Sun Microsystems of Canada in building SAMPOC II.

REFERENCES

Zeber, S. and Magar, A., 2002: Managing Identity and Access in the Defence Environment, Proc. of the 7th International Command and Control Research and Technology Symposium, September 2002.

Magar, A., 2003: Report on the Privilege Management Infrastructure (PMI) Proof-of-Concept (POC) Demonstration, DRDC Ottawa CR2003-003, January 2003.

Magar, A., 2004a: Report on the Enhanced Windows-based Warning Terms Separation Proof-of-Concept (POC) Demonstrator, DRDC Ottawa CR2004-058, April 2004.

Magar, A., 2004b: Report on Secure Access Management Proof-of-Concept (SAMPOC) II with Identity Management, DRDC Ottawa CR2004-122, June 2004.

CONCLUSIONS

SAMPOC I and II have successfully demonstrated that a practical integrated system solution for secure access management using commercial products and a content-based information security architecture is viable. They have also demonstrated the stability and flexibility of the architecture to support the evolution of commercial technology. Although there are still deficiencies to address before such a system could be deployed for operational use, most notably in the realm of evaluation and accreditation, the approach is sufficiently adaptable that it could be implemented in any environment. In particular, such a system could be used to enhance the capabilities of C4ISR systems to enforce need-to-know separation, and to support secure information sharing, in both national and multinational/coalition environments.

[4] This product is now available as an IBM Tivoli product.